Mississippi Department of Public Safety
Criminal Information Center (CIC)

MJIC Message Switch
Remote Server
Certification Test Procedures

Version 6.00 R02

April 12, 2018

TABLE OF CONTENTS

CHANGE LOG

Date	*Version*	*Change*
May 30, 2003	5.00	(New document)
July 21, 2008	5.00 R05	Revised for RFP 3569 for MCHS Mobile/Server Systems
June 11, 2010	5.00 R06	Revised test cases; added security document reference; added Two-Factor Authentication Tests for mobile devices
December 10, 2012	6.00 R01	Revised for directly-connected workstations and trusted servers (no longer supports terminals and terminal servers). Added test cases; deleted test cases for obsolete message types. Document restructured.
April 12, 2018	6.00 R02	Added message encryption test. Requires use of Encryption Header within Extended Message Header and use of Encryption Key Book. Moved Logon test to part of message encryption test. Terminology changed to "remote server". Removed directly-connected workstation section. Modified document title. Imbedded photos may now be included in messages from the remote server to the Message Switch. Added this to imbedded photos tests. (Support for this continues to be optional.) Added message encryption test for existing vendors who were previously certified. Merged remote server/MDT configuration tests in with remote server/workstation tests. Differences are noted in each test. Added mandatory Final Certification Step.

1.0 INTRODUCTION

Remote servers and their connected workstations/devices must be certified using the tests in this document.

The objectives of the certification tests are to verify that:

1. Messages can be entered at a workstation or other device and routed to the MJIC Message Switch and
2. Correct responses are generated, returned to the requestor at the workstation/device, and appropriately displayed.

2.0 REFERENCES

The following references apply to the interfaces described in this document. The applicable version is the version in effect at the time of certification. Contact the Criminal Information Center (CIC) to verify the correct versions of these documents.

1. Interstate Identification Index (III) Operational and Technical Manual, US Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Identification Division.
2. National Crime Information Center (NCIC) Operating Manual, US Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Identification Division.
3. Nlets Users Guide.
4. MCHS Security Policy.
5. CJIS Security Policy.
6. Datamaxx Message Processing Protocol® DMPP-2020 Interface Specification, Datamaxx Applied Technologies Inc. Version 9.0.
7. Datamaxx Standard Embedded Object® DSEO-2020 Object Processing in the Law Enforcement Environment Technical Specification, Datamaxx Applied Technologies Inc.
8. MJIC Message Switch Remote Server Interface Control Document.

3.0 GENERAL CERTIFICATION PROCESS

The general certification process is as follows.

1. The software used in the test must meet the interface requirements documented in the MJIC Message Switch Remote Server Interface Control Document, listed as reference 9 in section 2 of this document.
2. At least 2 weeks prior to the scheduled certification, the vendor must submit to Mississippi Department of Public Safety/Criminal Information Center (MDPS/CIC) a written description of the system to be certified. This description must include, at a minimum, a schematic of the system (i.e., servers, peripherals, network connections to MDPS/CIC, network connections to other systems, IP scheme, etc.) and the intended use of the system (i.e., inquiry only, data entry, both). For inquiry only stations, only a subset of the tests in section 4 through 6 will be performed.

   After certification, the vendor must send a notice to MDPS/CIC within 10 days of any installation at a customer site. The notice must provide a schematic of the installed system with an explanation detailing any changes from the configuration used by the vendor in the certification process. CIC will review the installed configuration. If there are any changes from the certified configuration, the customer site may not operate in a live mode until MDPS/CIC approves the configuration.
3. Vendors must contact MDPS/CIC at (601) 933-2601 to schedule certification and obtain user id(s), password(s), workstation/device id(s), server id, ORI(s), and IP address(es) to use for certification.
4. For certification, the vendor must install and operate a test configuration, including equipment and software, in the MDPS/CIC test environment. The test configuration must include all operating documentation, user manuals, or other materials that would normally accompany any subsequently purchased system. The test configuration must be either an exact replica of a system to be installed at a customer site or a typical/representative configuration. For remote servers, a test configuration is required that consists of the remote server and two attached workstations. For mobile data terminals, a laptop or desktop PC may be used to emulate the MDT client software. Two MDT client platforms are required for certification.

   MDPS/CIC certification test environment is located at 3891 Highway 468 West, Pearl, MS. All expenses for shipping, handling, installing, and testing the certification system will be borne by the vendor. Following certification, the vendor is responsible for de-installing and removing the certification system.

   MDPS/CIC will provide engineering support to answer questions regarding network connectivity for the certification test.
5. After vendor installation at CIC, MDPS/CIC will allow the vendor to perform preliminary testing of their system (after completing Test 4.1 and 4.2) using MDPS/CIC-provided user id(s), password(s), workstation/device id(s), ORI(s), and IP address(es). MDPS/CIC will also provide values for the messages listed in appendix C that may be used for the vendor's preliminary testing purposes. Although MDPS/CIC can provide limited support, it is expected that the vendor's product will have already been through a pre-ship test process based on all references listed in section 2 before being shipped to MDPS/CIC.
6. If the vendor is proposing multiple configurations, each configuration must be certified separately.
7. MDPS/CIC personnel will conduct the certification tests with the vendor's participation and make the final acceptance decision. MDPS/CIC will notify vendors of acceptance in writing within five (5) working days of completion of certification.
8. The test procedures will be performed using the software user interface that is part of the vendor product. The test procedures involve data entry resulting in specific messages being sent to the MJIC Message Switch and verifying that the expected response or responses are returned and displayed.
9. For test purposes, message responses must be displayed. Responses will be inspected for general format and content. If the vendor's software alters or synopsizes the response in a material way,

there must be a log or other mechanism to display the actual response sent to the workstation/device for certification verification purposes. MDPS/CIC personnel may also use other means to verify that the correct messages have been generated and the correct responses sent.

10. A test may be repeated at the discretion of MDPS/CIC to obtain timing information or to verify correct operation.
11. At its discretion, MDPS/CIC may request/perform additional tests for compliance with requirements in the ICD, or with NCIC, III, or Nlets documentation, or with CJIS and MCHS Security policies. MDPS/CIC may perform tests or request demonstrations of product features documented in the vendor's proposal or in the vendor's documentation.
12. The vendor may perform additional tests for MDPS/CIC, in addition to those called for in this document, in order to verify that their product will function correctly when installed at a customer site.

4.0 CERTIFICATION TESTS FOR REMOTE SERVERS

This section includes certification tests for workstations/devices that communicate through a remote server with the MJIC Message Switch.

- If a workstation/device connected to a remote server provides an inquiry only capability, only tests for inquiry messages are performed.
- If the device is a mobile data terminal (MDT), test 4.7 for two-factor authentication must be conducted. Otherwise, it is not required.
- For simplification in the text, the test messages in this section do not include the mandatory message prefix that is described in ICD section 4.2.1.

4.1 Message Encryption Test

This test verifies that the remote server properly encrypts all transmissions sent to the Messages Switch and properly processes all encrypted transmissions received from the Message Switch.

4.1.1 Test Preconditions

Vendor has coded and tested use of the Encryption Header (within the Extended Message Header) and use of the text version of the Encryption Key Book (using the sample provided in the DMPP-2020 Interface Specification Appendix A).

CIC preparation checklist in appendix B must be completed.

CIC has provided all items listed in Appendix A of this document to the vendor. This includes the Encryption Key Book. It is given to the vendor at CIC via an internet-based secure file exchange).

4.1.2 Evaluation Criteria

The evaluation criteria for this test are:

1. The Message Switch can successfully process the remote server's encrypted transmission.
2. The remote server successfully processes a response and displays it on a workstation/device.

4.1.3 Test Procedures

1. CIC sets the encryption flag on the Message Switch for the workstation/device.
2. Perform a Logon function that generates the following message to the Message Switch:

   `DOPS/MCH/`<*user id*>`/`<*password*>`/`<*workstation/device*>

where <*user id*>, <*password*> and <*workstation/device*> are those provided for certification testing by CIC.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

3. Enter an Nlets out-of-state Driver's License Query (DQ) that generates the following message: (Message #1 in appendix C.2.)

   `DQ.`<*ori*>`.`<*state other than MS*>`.TXTOLN/`<*driver's license number*>

Verify that a reasonable response is displayed on the workstation/device.

4.2 Logon, Logoff, and Change Password Tests

This test verifies the logon, logoff, and password change functions.

4.2.1 Test Preconditions

CIC preparation checklist in appendix B must be completed.

Test 4.1 must be completed.

CIC Tester must be logged on at the certification workstation/device.

4.2.2 Evaluation Criteria

The evaluation criteria for this series of tests are:

1. Each function is transmitted without error.
2. A complete and correct response is received for each function.

4.2.3 Test Procedures

Perform each of the following on a workstation/device that is connected to the remote server.

1. The Logon function was tested as part of the Message Encryption Test.
2. Perform a Logoff function at the workstation/device that generates the following message:

   `OPX`

Verify that a response is displayed on the workstation/device indicating the logoff has been accepted.

3. Repeat the Logon function in step 1 above.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

4. Perform a Change Password function that generates the following message:

   `DPWD/`<*new password*>`/`<*old password*>`/`<*confirm*>

where <*new password*> is a new password, <*old password*> is the current password and <*confirm*> repeats the <*new password*> value for confirmation purposes.

Verify that a response is displayed on the workstation/device indicating the password change has been accepted.

5. Repeat the Logoff function in step 2 above.

Verify that a response is displayed on the workstation/device indicating the logoff has been accepted.

6. Repeat the Logon function in step 1 above using the new password set in step 4.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

4.3 Law Enforcement Message Tests

This series of tests verifies that messages can be generated for the FBI NCIC and III systems, and for Nlets.

4.3.1 Test Preconditions

CIC preparation checklist item 5 in appendix B must be completed.

Tests in section 4.1 and 4.2 must be completed.

CIC Tester must be logged on at the certification workstation/device.

4.3.2 Evaluation Criteria

The evaluation criteria for this series of tests are:

1. Each of the messages is entered and transmitted to the Message Switch without error.
2. Data entry is efficient and clear.
3. Data entry and response times are both appropriate for an operational scenario.
4. A complete and correct response is received and displayed for each message.

4.3.3 Test Procedures for NCIC and III Messages

Perform each of the following tests on a workstation/device that is connected to the remote server. Regardless of the format in which the NCIC or III message is entered at the workstation, the remote server must generate a message as indicated below and forward it to the server.

1. Enter an NCIC Article Inquiry (QA) that generates the following message:

   `QA.<`*ori*`>.TYP/<`*article type*`>.SER/<`*serial number*`>`

Verify that the response is as expected.

2. Enter an NCIC Article Inquiry (QA) that generates the following message:

   `QA.<`*ori*`>.NIC/<`*nic number*`>`

Verify that the response is as expected.

3. Enter an NCIC Boat Inquiry (QB) that generates the following message:

   `QB.<`*ori*`>.BHN/<`*boat hull number*`>`

Verify that the response is as expected.

4. Enter an NCIC Query Boat (BQ) that generates the following message:

   `BQ.<`*ori*`>.REG/<`*boat registration number*`>`

5. Enter an NCIC Boat Inquiry (QB) that generates the following message:

   `QB.<`*ori*`>.NIC/<`*nic number*`>`

Verify that the response is as expected.

6. Enter an NCIC Gun Inquiry (QG) that generates the following message:

   `QG.<`*ori*`>.SER/<`*gun serial number*`>`

Verify that the response is as expected.

7. Enter an NCIC Gun Inquiry (QG) that generates the following message:

   `QG.<`*ori*`>.NIC/<`*nic number*`>`

Verify that the response is as expected.

8. Enter an NCIC Vehicle Inquiry (QV) that generates the following message:

   `QV.<`*ori*`>.LIC/<`*license plate number*`>`

Verify that the response is as expected.

9. Enter an NCIC Vehicle Inquiry (QV) that generates the following message:

   QV.<*ori*>.NIC/<*nic number*>

Verify that the response is as expected.

10. Enter an NCIC Vehicle Inquiry (QV) that generates the following message:

    QV.<*ori*>.VIN/<*vehicle id number*>

Verify that the response is as expected.

11. Enter a III Criminal History Inquiry (QH) that generates the following message:

    QH.<*ori*>.NAM/<*name*>.RAC/<*race*>.SEX/<*sex*>.DOB/<*date of birth*>.PUR/<*purpose code*>.
    ATN/<*attention*>

Verify that the response is as expected.

12. Enter a III Criminal History Record Request (QR) that generates the following message:

    QR.<*ori*>.PUR/<*purpose code*>.ATN/<*attention*>.FBI/<*fbi number*>

Verify that the response is as expected.

13. Enter a III Criminal History Record Request (QR) that generates the following message:

    QR.<*ori*>.PUR/<*purpose code*>.ATN/<*attention*>.SID/<*sid number*>

Verify that the response is as expected.

14. Enter a III Query Wanted Person Inquiry (QW) that generates the following message:

    QW.<*ori*>.NAM/<*name*>.SEX/<*sex*>.RAC/<*race*>.DOB/<*date of birth*>

Verify that the response is as expected.

15. Enter a III Query Wanted Person Inquiry (QW) that generates the following message:

    QW.<*ori*>.NIC/<*nic number*>

Verify that the response is as expected.

4.3.4 Test Procedures for Nlets Messages to Out-of-State Destinations

Perform each of the following tests on a workstation/device that is connected to the remote server. Regardless of the format in which the Nlets message is entered at the workstation, the remote server must generate a message as indicated below and forward it to the server.

1. Enter an Nlets out-of-state Driver's License Query (DQ) that generates the following message:

   DQ.<*ori*>.<*state other than MS*>.TXTOLN/<*driver's license number*>

Verify that the response is as expected.

2. Enter an Nlets out-of-state Driver's License Query (DQ) that generates the following message:

   DQ.<*ori*>.<*state other than MS*>.TXTNAM/<*name*>.DOB/<*date of birth*>.SEX/<*sex*>

Verify that the response is as expected.

3. Enter an Nlets out-of-state Driver's History Query (KQ) that generates the following message:

   KQ.<*ori*>.<*state other than MS*>.TXTOLN/<*driver's license number*>.PUR/<*purpose code*>.
   ATN/<*attention*>

Verify that the response is as expected.

4. Enter an Nlets out-of-state Vehicle Registration Query (RQ) that generates the following message:

   RQ.<*ori*>.<*state other than MS*>.TXTLIC/<*license plate number*>.LIY/<*license year*>.
   LIT/<*license type*>

Verify that the response is as expected.

5. Enter an Nlets out-of-state Vehicle Registration Query (RQ) that generates the following message:

   RQ.<*ori*>.<*state other than MS*>.TXTVIN/<*vehicle id number*>.VMA/<*vehicle make*>.
   VYR/<*vehicle year*>

Verify that the response is as expected.

6. Enter an Nlets out-of-state Person Query (IQ) that generates the following message:

   IQ.<*ori*>.<*state other than MS*>.TXTPUR/<*purpose code*>.ATN/<*attention*>.NAM/<*name*>.
   DOB/<*date of birth*>.SEX/<*sex*>.RAC/<*race*>.SOC/<*social security number*>

Verify that the response is as expected.

4.3.5 Test Procedures for Nlets Messages to In-State Mississippi DMV and MCHS

Perform each of the following tests on a workstation/device that is connected to the remote server. Regardless of the format in which the Nlets message is entered at the workstation, the remote server must generate a message as indicated below and forward it to the server.

1. Enter an Nlets In-State Mississippi DMV Driver's License Query (DQ) that generates the following message:

   DQ.<*ori*>.MS.TXTOLN/<*driver's license numbe*r>

Verify that the response is as expected.

2. Enter an Nlets In-State Mississippi DMV Vehicle Registration Query (RQ) that generates the following message:

   RQ.<*ori*>.MS.TXTVIN/<*vehicle identification number*>.VMA/<*vehicle make*>.VYR/<*vehicle year*>

Verify that the response is as expected.

3. Enter an Nlets In-State Mississippi Criminal History Repository (MCHS) Person Query (IQ) that generates the following message:

   IQ.<*ori*>.MS.TXTPUR/<*purpose code*>.ATN/<*attention*>.NAM/<*name*>.DOB/<*date of birth*>.
   SEX/<*sex*>.RAC/<*race*>.SOC/<*social security number*>

Verify that the response is as expected.

4. Enter an Nlets In-State Mississippi Criminal History Repository (MCHS) rap sheet request that generates the following message:

   FQ.<*ori*>.MS.TXTPUR/<*purpose code*>.ATN/<*attention*>.SID/<*state id number*>

Verify that the response is as expected.

4.4 Law Enforcement Message Data Entry Tests

This series of tests is intended to verify that all of the required message types and options can be properly entered. Optionally, CIC may also verify the responses to each of the message types.

4.4.1 Test Preconditions

Tests in section 4.1 and 4.2 must be completed.

CIC Tester must be logged on at the certification workstation/device.

4.4.2 Evaluation Criteria

The evaluation criteria for this series of tests are:

1. All required options for a message are provided.
2. Data entry is efficient and clear.
3. Data entry is appropriate for an operational scenario.
4. Optionally, a complete and correct response is received and displayed for each message.

4.4.3 Test Procedures

1. For each message listed in the NCIC Operating Manual, verify that:
   a. All message types can be entered.
   b. All mandatory and optional fields within each message type can be entered.
   c. Each field allows entry of a maximum length data value.
   d. Data entry is validated to insure that all mandatory fields are present.
   e. Data entry is validated so that only those combinations of fields allowed by the NCIC Operating Manual are allowed.
   f. Messages are sent and responses are received and displayed correctly. (Optional - at the discretion of CIC).

   Note that many of these NCIC messages involve data updates and hence may not be available on an Inquiry Only workstation/device.
2. For each message listed in the III Operational and Technical Manual, verify that:
   a. All message types can be entered.
   b. All mandatory and optional fields within each message type can be entered.
   c. Each field allows entry of a maximum length data value.
   d. Data entry is validated to insure that all mandatory fields are present.
   e. Data entry is validated so that only those combinations of fields allowed by the III Operational and Technical Manual are allowed.
   f. Messages are sent and responses are received and displayed correctly. (Optional - at the discretion of CIC).
3. For each query listed in the Nlets Users Guide, verify that:
   a. All message types can be entered.
   b. All mandatory and optional fields within each message type can be entered.
   c. Each field allows entry of a maximum length data value.
   d. Data entry is validated to insure that all mandatory fields are present.
   e. Data entry is validated so that only those combinations of fields allowed by the Nlets Users Guide are allowed.
   f. Messages are sent and responses are received and displayed correctly. (Optional - at the discretion of CIC).

4.5 Photos Imbedded in Messages Tests

This test is conducted only if the vendor is implementing one of the **optional** imbedded photos capabilities.

4.5.1 Test Preconditions

CIC preparation checklist item 5 in appendix B must be completed.

Tests in section 4.1 and 4.4 must be completed.

CIC Tester must be logged on at the certification workstation/device.

4.5.2 Evaluation Criteria

The evaluation criteria for this test are:

1. A complete and correct response, including imbedded photo(s), is received and displayed for each message.
2. The Message Switch receives a message with an imbedded photo(s).

4.5.3 Test Procedures

1. Enter a Mississippi DMV Driver License Query (DQ) that generates the following message: : (Message #1 in Appx C.4.)

    DQ.<*ori*>.MS.TXTOLN/<*driver's license number*>

Verify that an image of the driver's license photo is displayed in the response.

2. Enter an AM message with an imbedded photo: (Message #1 in Appx C.5.)

    AM.<*sender ORI*>.<*destination ORI*>.TXT<*newline*>

    This AM message includes a photo in DSEO-2020 format.

Verify that the Message Switch received the AM message with an imbedded photo.

4.6 Log Tests

This test verifies the requirements for separate logs that contain criminal history and non-criminal history data.

4.6.1 Test Preconditions

Tests in section 4.1 through 4.4, and 4.5 if certifying for imbedded photos, must be completed.

4.6.2 Evaluation Criteria

The evaluation criteria for this test are:

1. Ensure the logs are properly configured.

4.6.3 Test Procedures

Inspect the logs, which may reside at the workstation/device and/or the remote server to verify that:

1 Criminal history and non-criminal history data are kept in separate logs.

2. Both types of log information are either password protected or encrypted.

3. All law enforcement messages and response messages from the certifications test thus far have been logged.

4.7 Two-Factor Authentication Tests

This test is conducted if the device is a Mobile Data Terminal (MDT) or is an unsecure workstation that will perform III queries. In this case, two-factor authentication is required.

4.7.1 Test Preconditions

Tests in sections 4.1 through 4.6, including 4.5 if certifying for imbedded photos, must be completed.

CIC Tester must be logged on at the certification terminal/workstation.

4.7.2 Evaluation Criteria

The evaluation criteria for this test are:

1. Ensure login from a terminal/workstation is properly authenticated.

4.7.3 Test Procedures

Perform the following tests:

1. Verify that both valid credentials presented to the authentication server achieve valid login.
2. Verify that presenting 1st factor valid with 2nd factor invalid denies login.
3. Verify that presenting 1st factor invalid with 2nd factor valid denies login.
4. Verify that presenting 1st factor valid for User 1 and 2nd factor valid for User 2 denies login.
5. Verify that no credentials are passed in the clear.

4.8 Final Certification Step - MANDATORY

At the conclusion of tests at CIC, certification materials must be removed from the vendor's remote server. The CIC Tester must witness the following:

- Vendor deletes the Encryption Key Book. (CIC will send the Encryption Key Book to the vendor at the time of their first encrypted remote server installation.)
- Vendor deletes all CIC-provided user ids, workstation/device ids, remote server id, and ORIs.

5.0 ENCRYPTION CERTIFICATION FOR EXISTING VENDORS

This certification process is only for remote server vendors who have certified at CIC as of April 10, 2018.

5.1 Test Preconditions

In advance of the date of the test:

- Vendor has updated their remote server software to use the Encryption Header (within the Extended Message Header) and use the text version of the Encryption Key Book (using the sample provided in the DMPP-2020 Interface Specification Appendix A).
- Vendor contacts CIC to schedule the certification test. CIC and vendor determine the location of the test. (It may be possible to conduct this test from an existing installed site.)

In preparation for the scheduled test:

- If the test is conducted from an existing installed site, in addition to arranging this with the site, the vendor must provide a workstation/device to use for the tests.
- CIC provides a test workstation/device id and user id.

5.2 Evaluation Criteria

The evaluation criteria for this test are:

1. The Message Switch can successfully process the remote server's encrypted transmission.
2. The remote server successfully processes a response and displays it on a workstation/device.

5.3 Test Procedures

1. CIC sets the encryption flag on the Message Switch for the workstation/device.
2. Perform a Logon function that generates the following message to the Message Switch:

   `DOPS/MCH/<`*user id*`>/<`*password*`>/<`*workstation/device*`>`

where <*user id*>, <*password* and <*workstation/device*> are those provided for certification testing by CIC.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

2. Perform a Logoff function at the workstation/device that generates the following message:

   `OPX`

Verify that a response is displayed on the workstation/device indicating the logoff has been accepted.

3. Repeat the Logon function in step 1 above.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

4. Perform a Change Password function that generates the following message:

   `DPWD/<`*new password*`>/<`*old password*`>/<`*confirm*`>`

where <*new password*> is a new password, <*old password*> is the current password and <*confirm*> repeats the <*new password*> value for confirmation purposes.

Verify that a response is displayed on the workstation/device indicating the password change has been accepted.

5. Repeat the Logoff function in step 2 above.

Verify that a response is displayed on the workstation/device indicating the logoff has been accepted.

6. Repeat the Logon function in step 1 above using the new password set in step 4.

Verify that a response is displayed on the workstation/device indicating the logon has been accepted.

7. Enter an NCIC Vehicle Inquiry (QV) that generates the following message: (Message #10 in appendix C.1.)

QV.<*ori*>.VIN/<*vehicle id number*>

Verify that the workstation/device receives a normal response.

8. Enter a III Query Wanted Person Inquiry (QW) that generates the following message: (Message #15 in appendix C.1.)

QW.<*ori*>.NIC/<*nic number*>

Verify that the workstation/device receives a normal response.

9. Enter an Nlets out-of-state Driver's License Query (DQ) that generates the following message: (Message #1 in appendix C.2.)

DQ.<*ori*>.<*state other than MS*>.TXTOLN/<*driver's license number*>

Verify that the workstation/device receives a normal response.

10. Enter an Nlets In-State Mississippi DMV Driver's License Query (DQ) that generates the following message: (Message #1 in appendix C.3.)

DQ.<*ori*>.MS.TXTOLN/<*driver's license numbe*r>

Verify that the workstation/device receives a normal response.

11. Enter an Nlets In-State Mississippi Criminal History Repository (MCHS) Person Query (IQ) that generates the following message: (Message # 3 in appendix C.3.)

IQ.<*ori*>.MS.TXTPUR/<*purpose code*>.ATN/<*attention*>.NAM/<*name*>.DOB/<*date of birth*>.
SEX/<*sex*>.RAC/<*race*>.SOC/<*social security number*>

Verify that the workstation/device receives a normal response.

5.4 Final Certification Step - MANDATORY

If the test is conducted at CIC, perform the Final Certification Step as described in section 4.8.

If the test is conducted at a site the vendor must do the following:

- Delete the test workstation/device id and user id from the remote server.
- If the test is not successful, delete the Encryption Key Book from the remote server.
- Verify to the CIC that the specified items have been deleted.

APPENDIX A. MDPS/CIC-PROVIDED DATA

CIC will provide the following items to the vendor prior to certification testing.

- User id(s),
- Password(s),
- Workstation/device id(s),
- Remote server id,
- ORI(s), and
- IP address(es).
- Encryption Key Book (given to vendor at CIC via an internet-based secure file exchange).

At the conclusion of certification testing, the test ids and ORIs will be removed from the Message Switch.

APPENDIX B. MDPS/CIC CERTIFICATION PREPARATION CHECKLIST

In preparation for certification testing of a vendor's product CIC will:

1. Create the ids, etc. identified in appendix A on the MJIC Message Switch for the vendor's equipment configuration.
2. Assign IP address(es).
3. Identify the values to be used for the certification test messages listed in appendix C. These are used in the tests in section 4.3. Also, selected messages/values per appendix C are used in Test 4.1. (These values must be different than those provided to the vendor for preliminary tests. (See item 4 below.)

   Selected messages/values per appendix C are used for Encryption Certification for Existing Vendors in section 5.0.
4. Identify the values to be used for the preliminary test messages listed in appendix C. (See section 3.0 item 5.)

APPENDIX C. LIST OF CERTIFICATION TEST MESSAGES

The following messages are used in the test procedures. MDPS/CIC will provide values for parameters in angle brackets such as <*article type*>. One set of values will be provided for a vendor to use for preliminary testing (See section 3.0 item 5). Another set will be used in the certification tests.

C.1 NCIC/III Messages

1. QA.<*ori*>.TYP/<*article type*>.SER/<*serial number*>

2. QA.<*ori*>.NIC/<*nic number*>

3. QB.<*ori*>.BHN/<*boat hull number*>

4. QB.<*ori*>.REG/<*boat registration number*>

5. QB.<*ori*>.NIC/<*nic number*>

6. QG.<*ori*>.SER/<*serial number*>

7. QG.<*ori*>.NIC/<*nic number*>

8. QV.<*ori*>.LIC/<*license plate number*>

9. QV.<*ori*>.NIC/<*nic number*>

10. QV.<*ori*>.VIN/<*vehicle id number*>

11. QH.<*ori*>.NAM/<*name*>.RAC/<*race*>.SEX/<*sex*>.DOB/<*date of birth*>.PUR/<*purpose code*>.ATN/<*attention*>

12. QR.<*ori*>.PUR/<*purpose code*>.ATN/<*attention*>.FBI/<*fbi number*>

13. QR.<*ori*>.PUR/<*purpose code*>.ATN/<*attention*>.SID/<*sid number*>

14. QW.<*ori*>.NAM/<*name*>.SEX/<*sex*>.RAC/<*race*>.DOB/<*date of birth*>

15. QW.<*ori*>.NIC/<*nic number*>

C.2 Nlets Messages to Out-of-State Destinations

1. DQ.<*ori*>.<*state other than MS*>.TXTOLN/<*driver's license number*>

2. DQ.<*ori*>.<*state other than MS* >.TXTNAM/<*name*>.DOB/<*date of birth*>.SEX/<*sex*>

3. KQ.<*ori*>.<*state other than MS* >.TXTOLN/<*driver's license number*>.PUR/<*purpose code*>. ATN/<*attention*>

4. RQ.<*ori*>.<*state other than MS* >.TXTLIC/<*license plate number*>.LIY/<*license year*>. LIT/<*license type*>

5. RQ.<ori>.<*state other than MS* >.TXTVIN/<*vehicle id number*>.VMA/<*vehicle make*>. VYR/<*vehicle year*>

6. IQ.<*ori*>.<*state other than MS*>.TXTPUR/<*purpose code*>.ATN/<*attention*>.NAM/<*name*>. DOB/<*date of birth*>.SEX/<*sex*>.RAC/<*race*>.SOC/<*social security number*>

C.3 Nlets Messages to In-State Mississippi DMV and Criminal History Repository (MCHS)

1. DQ.<*ori*>.MS.TXTOLN/<*driver's license number*>

2. RQ.<*ori*>.MS.TXTVIN/<*vehicle id number*>.VMA/<*vehicle make*>.VYR/<*vehicle year*>

3. IQ.<*ori*>.MS.TXTPUR/<*purpose code*>.ATN/<*attention*>.NAM/<*name*>.DOB/<*date of birth*>. SEX/<*sex*>.RAC/<*race*>.SOC/<*social security number*>

4. FQ.<*ori*>.MS.TXTPUR/<*purpose code*>.ATN/<*attention*>.SID/<*state id number*>

C.4 Photos Imbedded in Response Messages

1. DQ.<*ori*>.MS.TXTOLN/<*driver's license number*>

   The response to this message includes a photo in DSEO-2020 format.

C.5 Photos Imbedded in Law Enforcement and Administrative Messages

1. AM.<*sender ORI*>.<*destination ORI*>.TXT<*newline*>

   This AM message includes a photo in DSEO-2020 format.